

The Microsoft 365 Migration Checklist

What to settle before anyone touches your email — and how to tell, the morning after, whether it actually worked.

Read this first

This is the checklist we work from ourselves. It is written so you can use it with any provider, including one that isn't us. If a supplier tells you half of this doesn't matter, that is useful information about the supplier.

A migration goes wrong in one of two ways. Either something is discovered on the night that should have been discovered three weeks earlier, or something quietly breaks and nobody notices for a fortnight — usually a scanner, an invoice alert, or a mailbox nobody logs into. Almost everything below exists to prevent one of those two.

1 · Before anyone quotes you

You cannot get an honest price without these. If a quote arrives without them being asked, it is a guess.

- ☐ Total number of mailboxes, split into **people** and **not-people** (info@, accounts@, sales@, noreply@)
- ☐ Size of the largest mailbox, and total size of all of them
- ☐ Where mail lives today — on-premises Exchange, a hosting panel, cPanel, Google Workspace, a reseller
- ☐ **Who controls the domain registrar**, and does someone in your building have the login
- ☐ Shared mailboxes, distribution lists and aliases, listed out
- ☐ Any mailbox that a **department** shares a password for — this is common and it changes the plan
- ☐ Archived mail: .pst files on desktops, an archive appliance, or a journaling setup
- ☐ Files as well as mail? A shared drive, a NAS, a server — or is this email only
- ☐ Mobile phones: how many, company-owned or personal
- ☐ Anything that **sends** mail without a person: scanners, the alarm system, the ERP, the accounting package, a website contact form

The last one is the single most common cause of “everything worked on Monday and the scanner stopped on Tuesday”. Walk the office and look at the machines.

2 · Licensing and tenant

- ☐ Which plan, and **why that plan** — you should be able to name the feature you are paying for
- ☐ Shared mailboxes do not need a licence in most cases. Check nobody has quoted you for licensing info@ and accounts@
- ☐ Where the tenant's data region is set, and whether that is acceptable to your bank, your auditor, or your parent company
- ☐ Who owns the subscription — **your company, in your name, on your payment method**. Not your IT provider's tenant with you inside it
- ☐ Global Administrator accounts: how many, who holds them, and whether there is a **break-glass account** written down and stored safely

- ☐ Annual or monthly commitment, and what happens to your data if you stop paying

A tenant registered in your provider's name is the single most effective form of lock-in in this industry. If you take one thing from this document, take this one.

3 · Domain and DNS

- ☐ Registrar login confirmed working **before** the migration date, not on the night
- ☐ Reduce the TTL on your MX records at least 48 hours ahead, so a rollback is fast if needed
- ☐ Record the current DNS as it stands today — a screenshot is fine, and it is your rollback plan
- ☐ MX, autodiscover, SPF, DKIM and DMARC planned on paper before anything changes
- ☐ SPF updated to include every system that sends on your behalf — mail platform, mailing tool, ERP, website
- ☐ DKIM enabled and **verified as signing**, not just switched on
- ☐ DMARC started at p=none so you can watch what happens before you enforce anything
- ☐ If your domain is with a reseller, confirm who can actually edit DNS. Some panels do not expose the records you need

4 · The cutover itself

- ☐ Cutover, staged, or hybrid — and the reason for the choice written down
- ☐ Date and time: after business hours, and **not** the night before month-end, payroll, or a deadline
- ☐ Who is on site, who is reachable, and one named person on the customer side who can make a decision at 11pm
- ☐ The coexistence window: during the switch some mail lands in the old system and some in the new. Agree how long that lasts and who checks the old one
- ☐ A rollback point, with the trigger for using it agreed in advance
- ☐ Old mail platform stays alive and paid for at least 30 days after. Do not cancel it the same week

5 · Data

- ☐ Mail, calendar and contacts — all three, per mailbox. Calendars are the ones people forget
- ☐ Recurring meetings and room bookings, checked after the move
- ☐ Delegate and send-on-behalf permissions rebuilt — these rarely survive on their own
- ☐ .pst files found, collected and imported. They are usually on individual desktops and nobody mentions them
- ☐ Shared drive or file server: what moves to OneDrive, what moves to SharePoint, what stays where it is
- ☐ Anything with a **long path or odd characters** in the filename identified before the copy, not during
- ☐ Retention: how long mail is kept, and whether anyone has a legal reason to keep it longer
- ☐ Backup. Microsoft replicates your data; that is not the same as backing it up. Decide who restores a mailbox somebody deleted six weeks ago

6 · Identity and access

- ☐ How passwords are set and handed over — and never by email

- ☐ Multi-factor authentication on, at minimum, every administrator and every finance mailbox
- ☐ A written plan for the person who will refuse MFA. There is always one
- ☐ Leavers: the process for disabling an account the same day someone leaves
- ☐ Former staff mailboxes converted to shared, not deleted, if anyone still needs the history

7 · Endpoints, and the things that are not people

- ☐ Outlook profiles on every desktop and laptop, and who does that work
- ☐ Mobile devices reconfigured, with someone in the office the next morning for the three people it does not work for
- ☐ **Scanners and copiers** that email documents — reconfigured and tested by scanning a document
- ☐ Alarm, CCTV or building systems that send alerts — tested by triggering an alert
- ☐ Accounting or ERP software that emails invoices — tested by sending a real invoice to yourself
- ☐ Website contact form and any automated notifications — tested by submitting the form
- ☐ Anything using SMTP relay: does it support modern authentication, or does it need a different approach

8 · How you know it worked

Do not accept “the migration is complete” without these, and do them yourself rather than watching someone else do them.

- ☐ Send and receive externally, from a mailbox that is not the administrator's
- ☐ Reply to an old thread and confirm the history is intact
- ☐ Open the calendar and confirm a recurring meeting three months out
- ☐ Scan a document from the copier and confirm it arrives
- ☐ Send an invoice out of the accounting system
- ☐ Check a shared mailbox opens for the people who need it
- ☐ Confirm mail flow from a mobile phone, on mobile data rather than office wifi
- ☐ Check the old platform for anything still arriving there

9 · What you should own at the end

Ask for these in writing. A provider who cannot produce them has left you dependent on them, whether or not that was the intention.

- ☐ Tenant name and the admin account, in your company's name
- ☐ A record of the DNS as it now stands
- ☐ The list of mailboxes, shared mailboxes, aliases and distribution lists
- ☐ Which systems send mail on your behalf and how they authenticate
- ☐ Licence count, renewal date and cost
- ☐ Where backups are, and who restores them

10 · The ones that catch people

From jobs we have actually run, not a textbook.

The reseller panel. Domains bought through a reseller sometimes hide the DNS controls you need, and delegation settings that should be in the admin centre are not exposed at all. Find this out weeks early, not on the night.

The mailbox nobody owns. Every company has an address that receives something important — a bank notification, a government portal, a supplier's invoices — that nobody has logged into for two years. Find it before you migrate, not when the bank calls.

The scanner. See above. It is always the scanner.

Calendar permissions. Two directors who could see each other's diaries on Friday cannot on Monday, and it gets reported as "the migration broke everything".

The shared password. A department all using one login for one mailbox does not survive MFA. Plan the change before, not during.

Cancelling the old system too early. Thirty days. It costs very little and it has saved more than one migration.

A note on what is coming

The UAE's electronic invoicing programme moves to mandatory phases from 2027. Where your mail and your documents live, and who controls that tenant, becomes materially harder to change once invoicing is wired into it. If a migration is on your list at all, doing it before that work starts is considerably easier than after.

Regulatory dates as of August 2026. Confirm current requirements with the Ministry of Finance or your tax adviser — Ontrac is an IT provider, not a tax agent or an accredited service provider.

If you want a hand

We run these migrations across Dubai and the Emirates. We will also happily look over a plan you have had from someone else and tell you what is missing, at no charge, because a badly run migration usually becomes somebody's emergency and we would rather it did not become yours.

Ontrac Business Solutions FZE

+971 (0)4 424 0157 · dxbops@ontrac.biz · ontrac.biz

PO Box 27558, Dubai, United Arab Emirates

Licence No. 14092 · TRN 100350374300003

Every design we deliver is documented and transferable. If you move on, you leave with everything.